タイトル：STPA 分析での HCF（ハザード因果要因）から LS(損失シナリオ）への変遷の理由

まえがき

2011 年に発刊した STAMP 理論の教科書（Engineering a Safer World,日本語訳：システム理論による安全工学、共和出版、2024 年）では、STPA のなかで「**HCF**（Hazard Causal Factors,ハザード因果要因)」という言葉が使われている。しかしながら、その後の STPA の手順を具体的に説明したハンドブック（https://psas.scripts.mit.edu/home/get_file2.php?name=STPA_Handbook_Japanese.pdf）では、これが、**LS**(Loss Scenarios,　損失シナリオ)という言葉に置き換えられている。2015 年に Nancy Leveson 教授が来日して IPA で講演された際の議論で、「この HCF という表現は事故の原因をチェックリストのように扱ってしまうことにつながるので、間違った表現であった」と述べていたことが印象に残っている。本稿ではその理由をもう少し丁寧に説明したい。

STPA の手順

STPA は、安全目標（損失の定義)、安全制御構造のモデル化、非安全コントロールアクションの識別、損失シナリオの識別という 4 つのステップからなっている。この 4 番目のステップの説明に、前記「システム理論による安全工学」の「8.4.1　因果関係シナリオの識別」の中の図 8.6 では、以下の図が用いられている。この図の説明で「因果要因、Causal Factors」という言葉が使われ、これが HCF の語源となっている。IPA で STAMP に関する委員会を主宰しており、当初はこの図に従って事故シナリオを導出する際の参考 HCF を「ガイドワード」と呼んでいたが、冒頭述べたように「HCF という表見は間違っていた」というコメントに従って、「ヒントワード」と呼ぶことにしている。

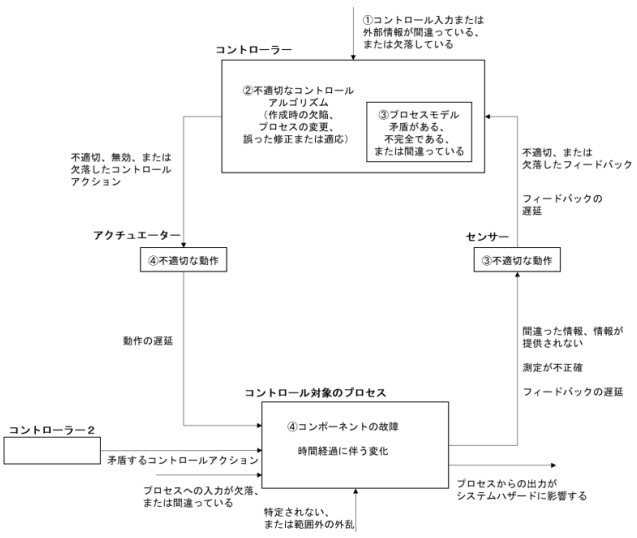

図 8.6　ステップ 3 でシナリオを作成するときに考慮すべき**因果要因**

一方、2018 年に発行された STPA ハンドブック（https://psas.scripts.mit.edu/home/get_file2.php?name=STPA_Handbook_Japanese.pdf）では、この第 4 ステップが、損失シナリオ（LS）の識別として明示化され、そのための参考図として以下のフィードバックループの図が示されている。図のタイトルは、「考慮すべき二つのタイプのシナリオ」となっている。「何故非安全なコントロールアクションが起こるのか」、「何故コントロールアクションが不適切に実行されるのか、または実行されないのか」というように、指示を出す側と受け取る側に大別して、抽象化したヒントになっていることが分かる。ハンドブックでは、この二つのタイプのシナリオをさらに、下記のような二つの図で詳細化して説明している。

図 2.18：非安全なコントロールアクションが、(1)非安全なコントローラの動作及び(2)不十分なフィードバック及び他の入力、によって引き起こされる

図 2.19： コントロールプロセスに影響を与えるような 1）コントロール経路と 2）他の要因を表す一般的なコントロールループ

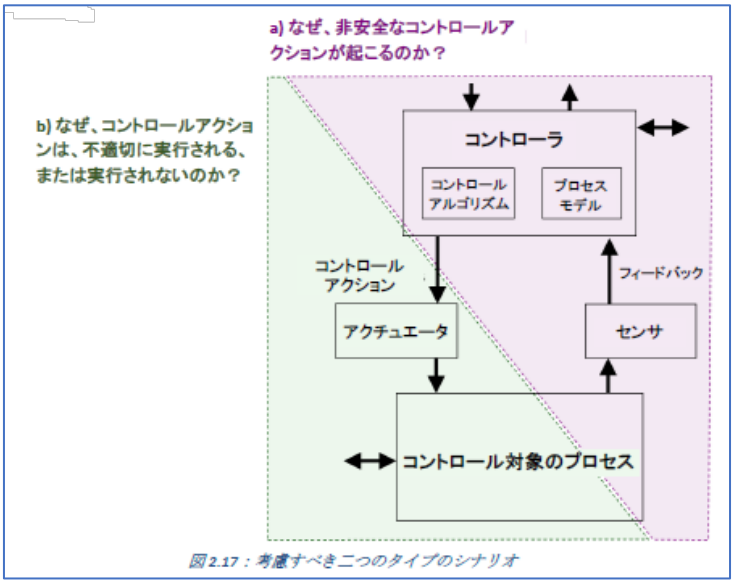

図 2.17：考慮すべき二つのタイプのシナリオ

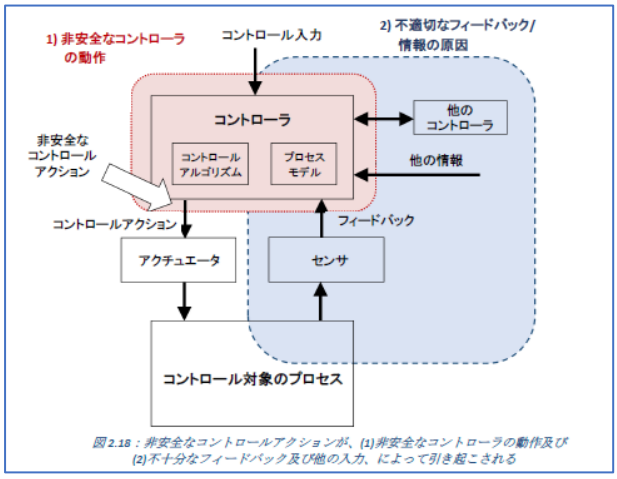

図 2.18：非安全なコントロールアクションが、(1)非安全なコントローラの動作及び(2)不十分なフィードバック及び他の入力、によって引き起こされる

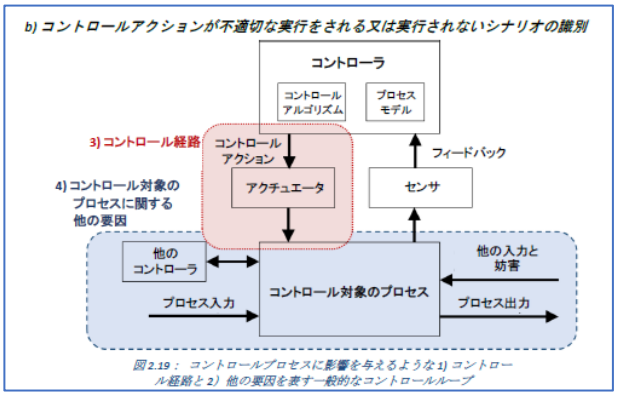

図 2.19： コントロールプロセスに影響を与えるような 1) コントロール経路と 2）他の要因を表す一般的なコントロールループ

このハンドブックでは、これらのシナリオの説明として以下のような記述がある。（下線は著者が追加）

『共通のミスを防止するためのヒント

共通のミスの多くは、シナリオよりもむしろ、個々の因果関係要因を識別することにあります。例えば、「ホイール速度センサの故障」、「ホイールの速度フィードバックが遅れる」、「電源喪失」のような要因のリストを作成したくなるかもしれません。シナリオのコンテキストを超えて個々の要素をリストにすることの問題は、複数個の要因がどのように相互作用を及ぼすのかを簡単に見落としてしまうことにあります。また、間接的に UCA やハザードにつながる、つまらないことではないが明白にわからない要因を見落とすことになりますし、これらの要因の組み合わせがハザードに至ることを考えなくなるでしょう。単一の要因群を考慮することは、本質的に、コンポーネントの単一故障だけを考慮するという FMEA になってしまいます。 』

下線部で示した部分に STAMP 理論の思想がよく表されている。個々の要素をリストにする（チェックリスト化）ことの問題点と、複数個の要因の相互作用を見ることの大事さを主張しており、FTA や FMEA のような従来の事故分析手法との違い（パラダイムシフト）を明確にしている。FTA で用いられる共通原因故障（CCF、Common Cause Failure）と、今回の複合的な要因の分析では、おおきな違いがあることも指摘しておく。CCF は、複数の安全装置に共通の電源が使われるようなハードウェアに特化した共通事象を主に考えていることに対して、STAMP での複合的な要因分析では、機械の故障、人の誤操作、組織の硬直化のように異なるコンポーネント間の不適切な要因が重なって起こる事故を対象にしている。

この具体例として前記「システム理論による安全工学」の中からスペースシャトルの墜落事故の事例を引用しておく。機械と人・組織の絡まりあった複雑な事故の分析と再発防止には、STAMP のような包括的で複合的な安全分析が必要とされることが良くわかる事例である。（下線は著者が追加）

『**チャレンジャー号**（Challenger）の事故調査で連鎖の探索が O リング（オーリング、訳注：高温ガスの漏れを防ぐためのフィールドジョイントのシール）の故障で止まってしまった場合、その特定の設計の欠陥を修正しても、将来の事故につながるシステミックな欠陥がなくなるわけではない。**チャレンジャー号**に関しては、そのようなシステミックな問題の例として、問題のある意思決定とそれにつながる政治的・経済的プレッシャー、問題報告の不備、傾向分析の欠如、「沈黙した」または効果のない安全プログラム、コミュニケーションの問題などが挙げられる。

（　中略　）それから 20 年後、またもやスペースシャトルが失われた。**コロンビア号**の事故（断熱材がオービターの翼に衝突）の直接原因は**チャレンジャー号**の事故と大きく異なるが、システミックな因果要因の多くは類似しており、**チャレンジャー号**の事故後にこれらの要因が十分に修正されなかった

（　中略　）事故がなぜ発生したのかの説明を提供するために、事故に関与した**すべての要因**を識別し、これらの要因間の関係を理解することに重点を置いている。その説明をもとに、将来の損失を防止するための提案をすることができるのである。』

O リングの機械故障以外の組織要因まで事故原因の分析がなされているが、安全対策として、特に組織要因への対策が十分になされていなかったと書かれているが詳細までは不明である。コロンビア号の事故まで 20 年の歳月が流れており、スタッフの代替わりなどによる経年劣化の可能性もある。STAMP に

よる包括的な安全分析と運用体制の経年変化の分析などが大切であることが分かる。

あとがき

機械と人・組織の絡まりあった複雑な事故の分析と再発防止には、STAMP のような包括的で複合的な安全分析とそれに基づく対策が必要であることを述べた。

具体的事例として、チャレンジャー号の墜落事故と 20 年後に再度墜落したコロンビア号の事故を引用した。これらの間で、直接原因は大きく異なるが、システミックな因果要因の多くは類似しており、直接原因だけでなく、システミックな因果要因まで含めた複合的な対策が必要とされる具体例である。多くの事故報告では表層的な直接原因だけでなく、それをさらに深めた根本原因分析（RCA）まで行って再発防止対策を行っているが、STAMP（特に CAST）では、さらに広い視野でシステミックな因果要因を洗い出し、それらの複合的な因果関係の理解から再発防止策を検討している。割り切った言い方になるが、FTA→RCA→CAST という順に、分析を深めたり（RCA)、広げたり（CAST）することで、複雑システムの安全をより高めているといえよう。

HCF から LS という呼び方の変遷の背景には、上記のように、STAMP の思想にかかわる大事な考え方が隠されているのである。

以上（2025/10/19　兼本　茂）